

Leviathan: Command and Control Communications on Planet Earth



Kenneth Geers

2501

Kevin Thompson

Threat Analyst, FireEye

Abhishek Pidwa

Data Analyst Intern, FireEye

Black Hat Las Vegas 2014

Abstract

Every day, computer network attackers leverage a Leviathan of compromised computer infrastructure, based in every corner of the globe, to play hide-and-seek with network security, law enforcement, and counterintelligence personnel.

This presentation draws a new map of Planet Earth, based not on traditional parameters, but on hacker command and control (C2) communications. The primary data points used in this worldwide cyber survey are more than 30 million malware callbacks to over 200 countries and territories over an 18-month period, from January 2013 to June 2014.

First, this talk covers the techniques that hackers use to communicate with compromised infrastructure across the globe. The authors analyze the domains, protocols, ports, and websites used for malicious C2. They explain how covert C2 works, and how attackers keep their communications hidden from network security personnel.

Second, this talk looks at strategic impact. The authors examine relationships between the targeted industries and countries and the first-stage malware servers communicating with them. Traffic analysis is used to deduce important relationships, patterns, and trends in the data. This section correlates C2 communications to traditional geopolitical conflicts and considers whether computer network activity can be used to predict real world events.

In conclusion, the authors consider the future of this Leviathan, including whether governments can subdue it – and whether they would even want to.

About the Data in this Paper

For this whitepaper, our team analyzed first stage command and control (C2) malware callbacks from FireEye clients around the world. Here is a brief description of our data set:

- 30+ million total callbacks
- 1+ million unique callbacks
- 20+ industry verticals targeted

This information comes from the FireEye Dynamic Threat Intelligence (DTI) cloud, which consists of attack metrics that are voluntarily shared back to FireEye from its clients, who are chiefly large corporate and government organizations.

It is important to note that these are real world data points, and this is not a theoretical analysis. These callbacks were all part of active computer network attacks in 2013 and 2014. Some of them were associated with relatively common malware, but many others were part of highly targeted attacks.

FireEye appliances are normally positioned behind firewalls, intrusion detection systems (IDS), proxies, web filters, and anti-spam technology. In other words, the malware associated with these callbacks successfully bypassed all of those other security tools, which serves to dramatically increase the reliability and credibility of our attack data. These are the types of attacks that corporations around the world are dealing with on a daily basis. None of the domains discussed in this paper were discovered by reverse engineering malware samples, domain generation algorithms, or domains suspected to have been registered by known bad actors.

Introduction

Planet Earth today benefits from the existence of cyberspace, which allows humans to communicate faster and farther than any previous generation could have imagined. However, malicious code, or malware, currently threatens the integrity of cyberspace. Malware is so easy to disseminate that malicious attackers have built a worldwide malware infrastructure that spans every country and territory on Planet Earth.

This Black Hat white paper analyzes millions of first-stage malware “callbacks” – the command and control (C2) communications between attacker and victim networks – over an 18-month period, from January 2013 to June 2014. The authors demonstrate that simple traffic analysis can be used to discover not only that this Leviathan exists – and can be used by attackers to thwart identification by security administrators, law enforcement, and counterintelligence – but that it is also possible to discover important patterns of activity, and significant trends in cyber security.

At the strategic level, this white paper can help national security decision makers understand the magnitude of the world’s current computer security challenges by demonstrating how big this Leviathan really is. At the tactical level, this analysis can help network security administrators by demonstrating that it is possible to examine network security and national security events in tandem, in order to gain a better understanding of both.

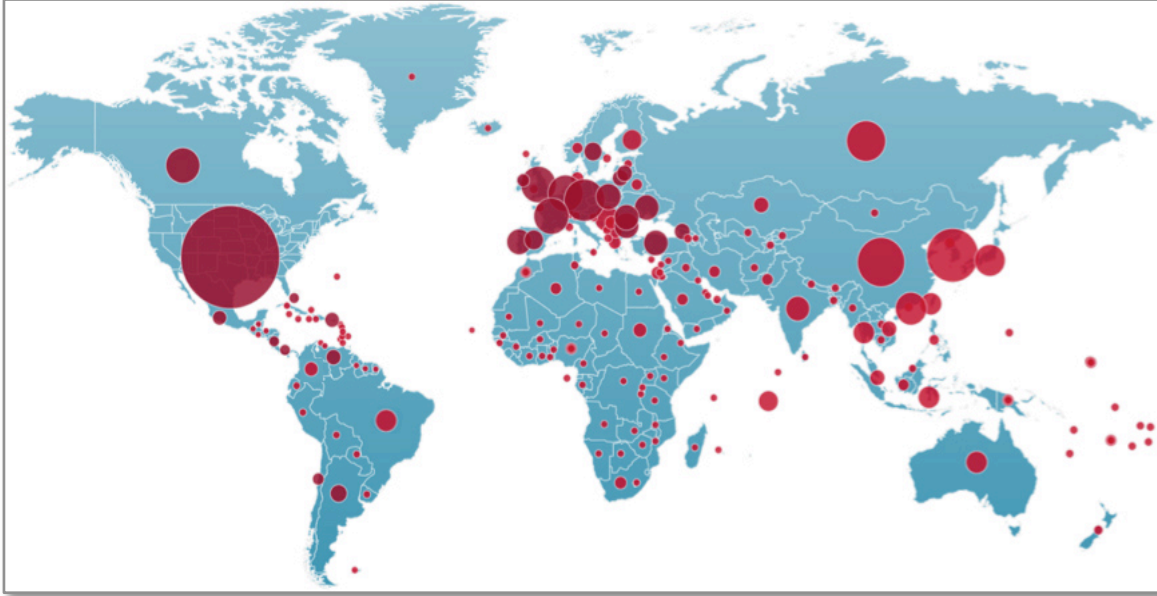
In this paper, the authors do not attempt to attribute the hacker activity observed to any real world actor, or to guess the precise motives of the attackers behind them. Within such a large number of callbacks, there are likely to be lone hackers, “patriotic hackers”, cyber criminals, host nation government operations, and operations initiated by other nations.

Instead, this paper employs “traffic analysis” in an attempt explore some preliminary hypotheses based on traffic volume, direction, and/or frequency. One of the most vexing challenges in cyber security today stems from poor attribution – or the “anonymous hacker” problem. However, in traffic analysis, it is not always necessary to know the exact content of any observed message, or even the identity of the sender, in order to draw some basic conclusions. The same principle applies to reporters who count the number of pizza deliveries to the Pentagon in the middle of the night; if the number rises dramatically without any obvious warning, something, somewhere in the world, may be happening that would be of interest to their readers.

In writing this paper, the authors understand that first stage C2 traffic is just one piece of a much larger puzzle. However, they also believe that this data set is large enough that it can and does shed new light on the fast-growing connection between network security and national security.

Worldwide malware ecosystem

Let's begin by looking at a world map of malware, represented by over 22 million C2 communications from Jan–Dec 2013.



A map displaying the locations of all the physical crime that happens in the world during the span of one year tends to shock most people when they see how widespread the problem is. We hope that this analysis will do the same for cyber attacks by demonstrating just how common they are.

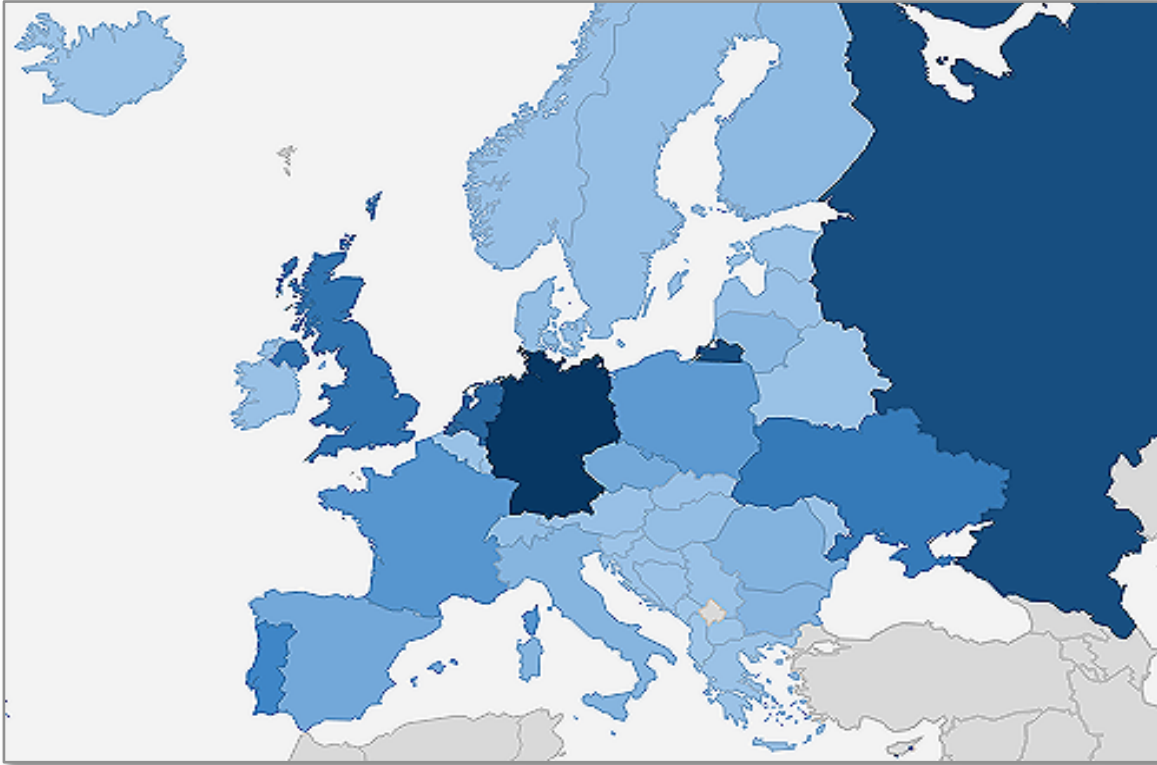
The U.S. is currently home to a significant portion of the world's malware infrastructure, or 24.1% of our observed callbacks in 2013. Internationally, the most significant clusters of activity were in Europe and Asia. Nearly all of Africa, and even remote places such as the Falkland Islands, Greenland, St Helena, French Polynesia, and Åland are also now home to compromised networks.

The global nature of malware callbacks suggests that the existence of so many compromised computers within any given jurisdiction can pose a substantial threat to national security. However, at the same time, they also give local law enforcement, counterintelligence, and foreign intelligence services the opportunity to conduct aggressive computer network operations against foreign attackers resident on or transiting their networks.

What is the immediate takeaway from this world map of malware? It is that cyber attackers can and do operate from literally any point on Planet Earth.

European C2 server heatmap

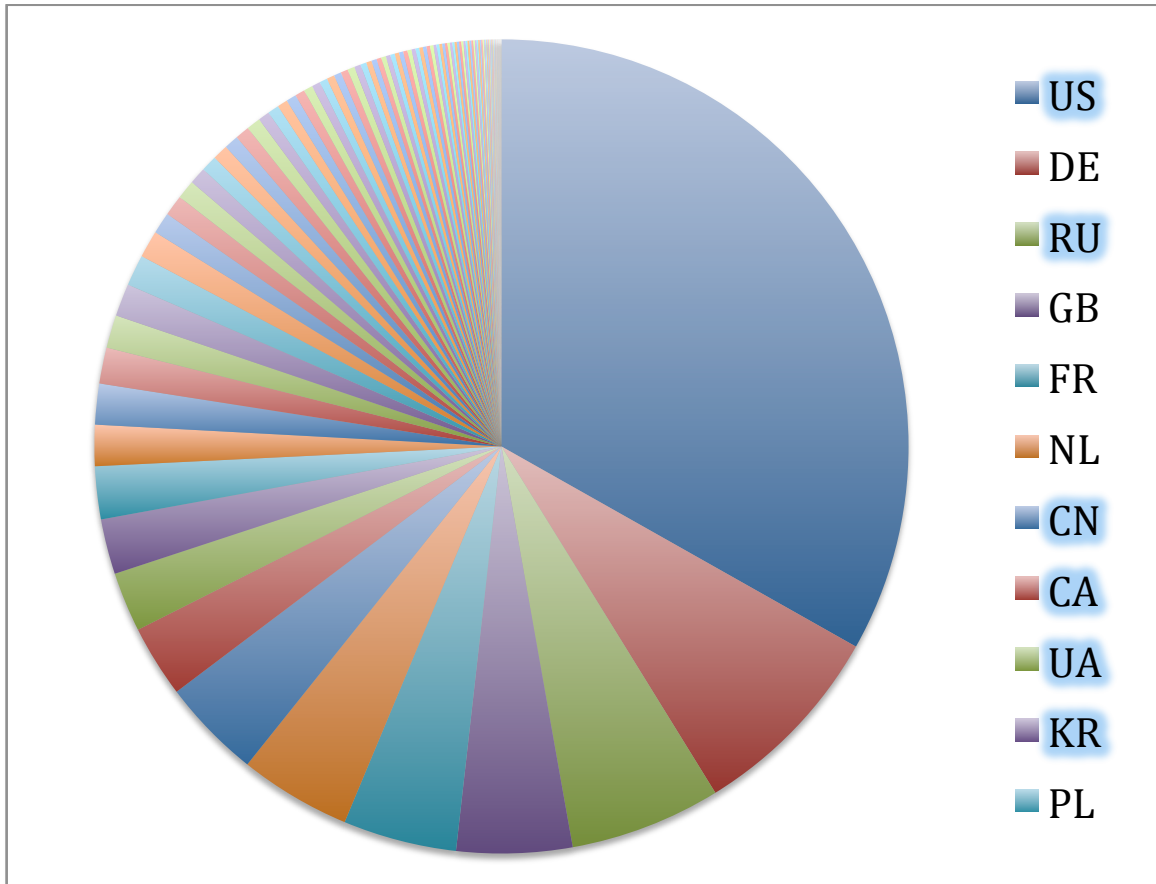
Let's zoom in on one continent. Here is a heat map of C2 servers in Europe during the first six months of 2014.



Currently, the two biggest destinations for malware callbacks to Europe are in Germany and Russia.

European callback destinations

The pie chart below turns this data set around, and examines the countries that hosted C2 servers and received callbacks from FireEye clients in Europe between January 2013 and June 2014.

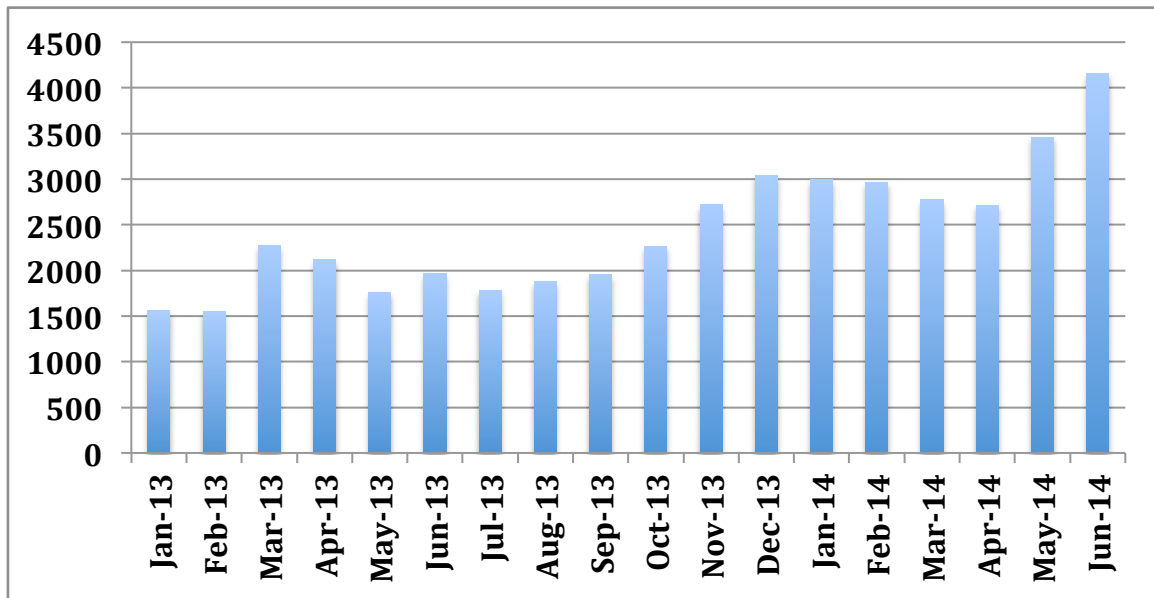


Four of the top ten countries were members of the European Union (EU), but six of them were outside of the EU – with the U.S. and Russia topping the list.

Growing dataset (*unique* EU callbacks)

In 2013 alone, FireEye collected and analyzed over 22 million callbacks. The dataset explored in this paper runs into July 2014. On average, the total number of observed callbacks per month varied between 1.2 – 2.2 million.

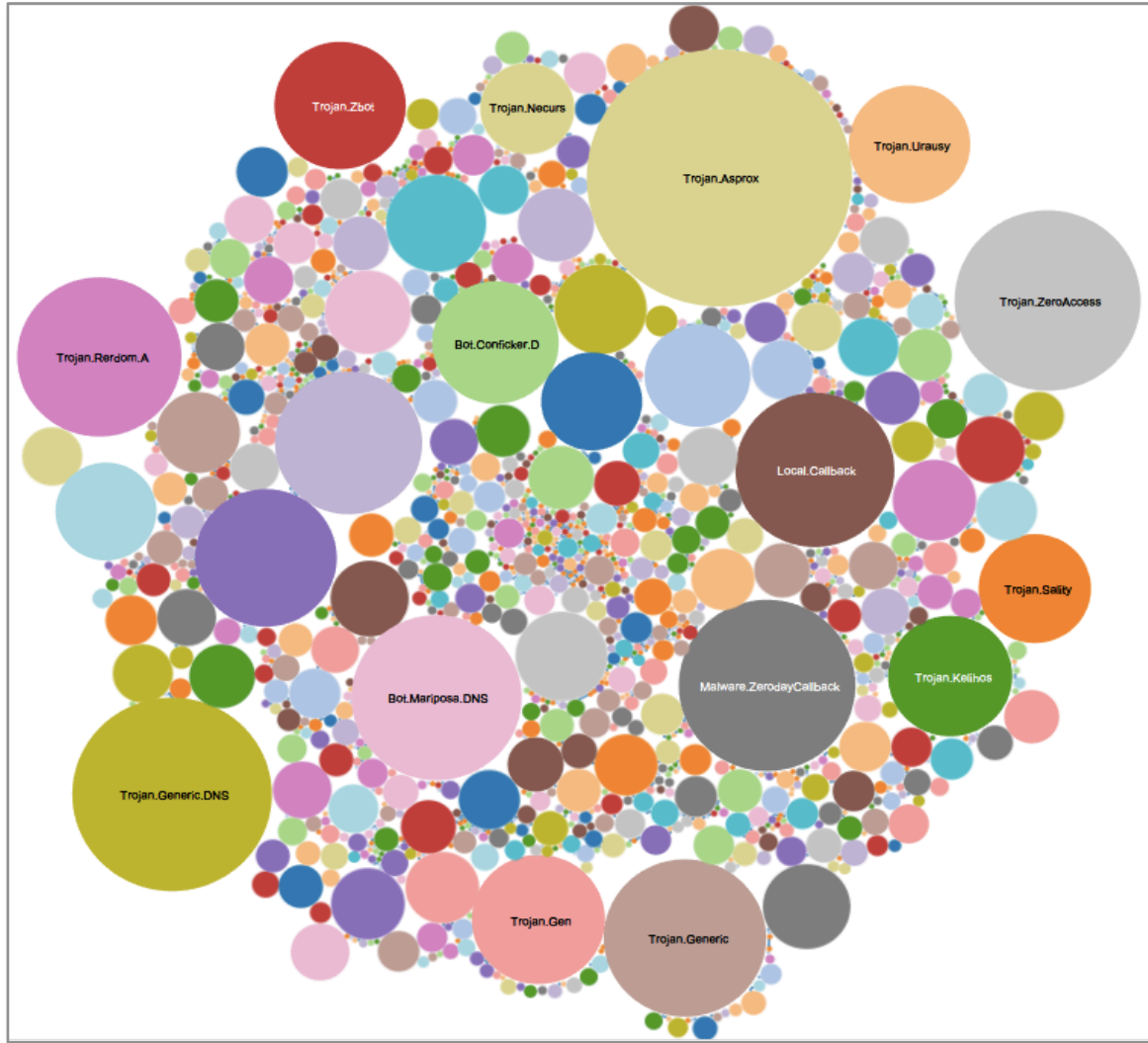
However, in order to make better sense of such overwhelming numbers, one way we have cut this huge number down is to simply pair unique victim networks with unique malware families calling out to remote C2 servers. The graph below is based on these metrics.



As you can see, the number of unique callbacks we have had available for analysis has grown considerably over the past 18 months.

C2 malware signatures

The bubble chart below shows 1,662 malware families we observed calling back from our clients to remote C2 servers during 1H 2014.



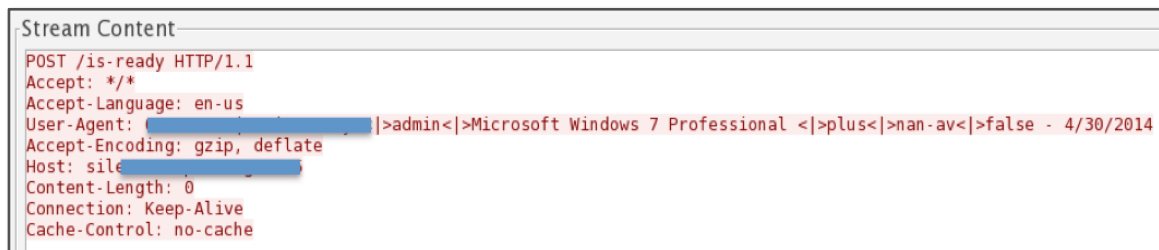
Although some common malware programs are responsible for the lion's share of C2 communications (keeping in mind that all of these were successful compromises), the most advanced actors are likely to be found among the lesser-known, smaller circles hiding somewhere in the middle of the chart.

Tactics, techniques, and procedures

At a technical level, a “callback” is a covert communication from an infected victim computer to an attacker’s command and control (C2) server, and it is one of the most reliable indicators of computer compromise.

The first callback usually occurs as soon as a computer vulnerability has been successfully exploited by an attacker, and they will continue in some form or fashion until the computer has been disinfected or taken offline. In the first instance, a callback is likely to include basic technical information about the newly compromised system, such as Internet Protocol (IP) address, computer name, operating system, username, password, user ID, country location, security software, whether a webcam is available, etc.

Callbacks are typically hidden within normal streams of communication, such as HTTP (web data) packets – which are almost always allowed through firewalls, because they are supposed to be user-initiated. In the example below, a malware program is informing a C2 server that it has been installed on a Windows 7 workstation, and that it did not detect the presence of anti-virus software.



```
Stream Content
POST /is-ready HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: [redacted] |>admin<|>Microsoft Windows 7 Professional <|>plus<|>nan-av<|>false - 4/30/2014
Accept-Encoding: gzip, deflate
Host: sile
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
```

Below, here is an example of an encoded callback from the remote access hacker tool called njRAT (its name at FireEye is “Backdoor.APT.LV”).

```
lv|'|
2YLZgNin2KrZgNmEINmF2YDY09is2YDZiNixXzQwMENENTew|'|
Remote PC|'|admin|'|2013-04-22|'|USA|'|Win XP Professional SP2
x86|'|No|'|0.5.0E|'|..|'|
QzpcV0IORE9XU1xzeXN0ZW0zMlxjbWQuZXhl|'|[endof]
```

This information includes a malware campaign name created by the attackers, a NetBIOS name, username, date, victim location, operating system, webcam availability (yes or no), malware version, and the encoded title of Windows foreground window (e.g. C:\WINDOWS\system32\cmd.exe). All of this information can be put into the attacker’s database for future use.

At this point in the game, with a reliable line of communication established with the newly compromised computer, the attacker can provide additional commands, including:

- to download more malware,
- to conduct deeper network reconnaissance,
- to search for specific files or information,
- to manipulate software or hardware management controls, and/or
- to exfiltrate stolen data.

In due course, the attacker will want to move laterally through the victim's network – and this process will also be managed via callbacks.

C2 dissection

Attackers do not communicate with their victims directly, but employ numerous layers of deception and misdirection. Thus, in most cases, the location of the first stage callback is not the attacker's true location, but just a small part of the attacker's malware infrastructure, which can be based anywhere in the world. Furthermore, an attacker seeks to craft his or her communications to appear innocuous, so as not to raise the suspicion of security administrators. However, reviewing these stage one communications over the course of many months has given us the opportunity to undertake a strategic analysis of this problem.

Below, we list a few basic ways that attackers can trick network defenders.

Domains vs. IP addresses

The first and easiest way to divide C2 communications is by domain name vs. Internet Protocol (IP) address. In 2013, roughly 54% of the malware C2 we examined replaced domain names with IP addresses before sending the first stage callback.

Port numbers

Callbacks use a variety of port numbers outside of the traditional port 80 or 8080, which is typical for most HTTP traffic. In 2013, we saw victim machines send malicious C2 to 33,697 different port numbers, or nearly 50% of the available ports assigned by Internet Engineering Task Force (IETF) process for standards-track protocols. The most frequently used ports were under 5000, but there was large concentration of malware using port numbers in the 15k to 16k range, suggesting that many corporate and government networks were infected by a malware version called ZeroAccess and using these high port numbers for peer-to-peer communications. In the <1k range, we found very limited usage in the 400s, which is often used for Secure Sockets Layer (SSL). An even smaller amount of callbacks used ports in the 50s range, which is normally reserved for Domain Name System (DNS) lookups. Below 100, the vast majority of malware used Transmission Control Protocol (TCP) port 80, most often used by Hypertext Transfer Protocol, or standard Web traffic. The heavy use of port 80 highlights the difficulty of preventing malicious C2 – no organization can adequately monitor this port, much less block it.

Vertical Analysis: Education

We divided our callbacks into 18 industry verticals, including Education, Government, High-Tech, Finance, Energy, and more. For 2013, one of our most interesting findings was that although Education was #3 on the list of total callbacks by vertical, Education sent by far the highest number of unique callbacks – almost twice as many as Government or High-Tech (#2 and #3 on the list). We believe the reason for this could be a volatile mixture of high intellectual property value

combined with a relatively open culture, collaborative culture. The Healthcare vertical was highest on the list of total callbacks, likely due to extremely “noisy” malware calling out many times in succession.

Furthermore, we discovered that the Education vertical (the .edu domain) was also the recipient of many first-stage callbacks from other verticals. As part of our analysis, we checked to see which specific academic departments received the callbacks – the most frequent was the library, and the second was computer science.

☺

Vertical Analysis: Government

Government domains from over twenty countries were also the recipients of first-stage C2 communications. Africa, Asia, and South America were the regions that had the most government domains used by attackers for callbacks in 2013.

Domain Analysis

To make their C2 communications appear innocuous to security administrators, attackers use “spoofed” domains in an attempt to lull network defenders into a false sense of security. Often, they seek to blend C2 data into normal corporate network traffic, which can even be sent to entirely legitimate websites for later retrieval.

For this analysis, we saw hackers use just about every trick in the book. We identified the use of spoofed domains that were similar to the top five most visited websites according to Alexa’s Top 100:

- 200+ domains spoofing Google (e.g. “gooqle”);
- 200+ domains spoofing FireFox (e.g. “fireofx”);
- 50+ domains spoofing Facebook (e.g. “faceboak”);
- 100+ domains spoofing Microsoft (e.g. “microsocft”);
- others included “yahoos”, “youtubeta”, and “windosw”;
- and don’t forget the lesson of the [dingo and her baby](#), in which the attacker spoofed the victim’s domain.

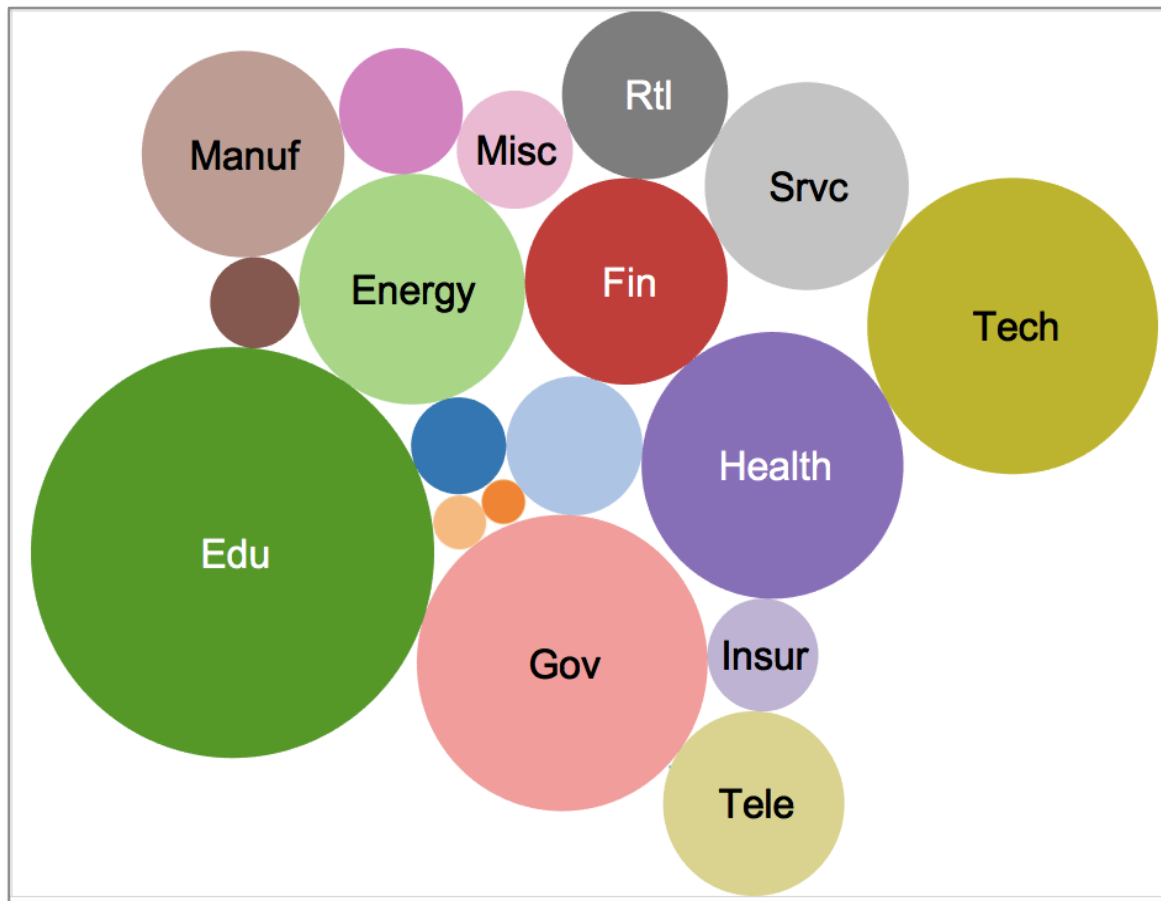
Hiding in plain “site”

Every malware program can have its own unique way of passing secret information to a C2 server. Covert communications are not limited to Web traffic – they come in virtually any disguise, and can use any protocol or filetype for transmission. Secret information can even be hidden (encoded and/or encrypted) within non-secret data, a practice known as steganography. For example, this image of North Korean stamps, at one time, also contained malicious, executable code.



Every industry vertical owned

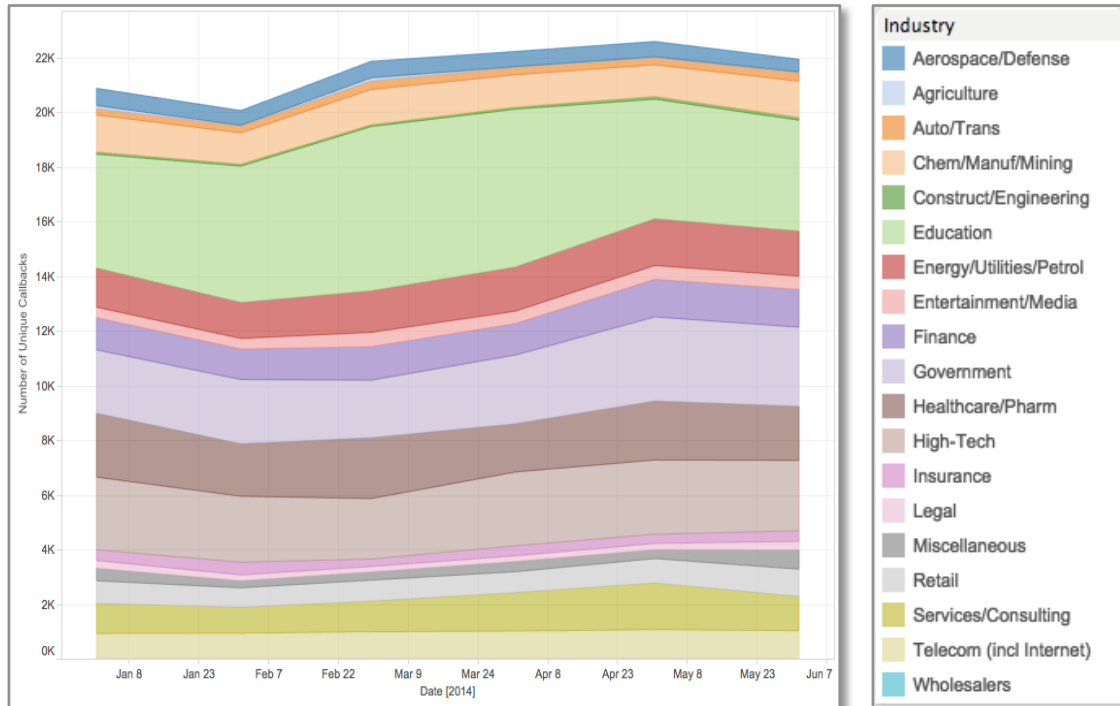
This bubble chart was generated from our 2014 data set. It sorts 1H 2104 callback data by compromised industry vertical. The circles represent the volume of malware callbacks per vertical over a six-month timeframe.



Malware is likely to be found in countries where there is significant intellectual property to steal, or national security-related information to discover. Further, we believe that the Education vertical is often exploited by hackers due to a healthy mix of large networks, cutting edge intellectual property, and an relatively open networking culture.

Callbacks: ebb and flow

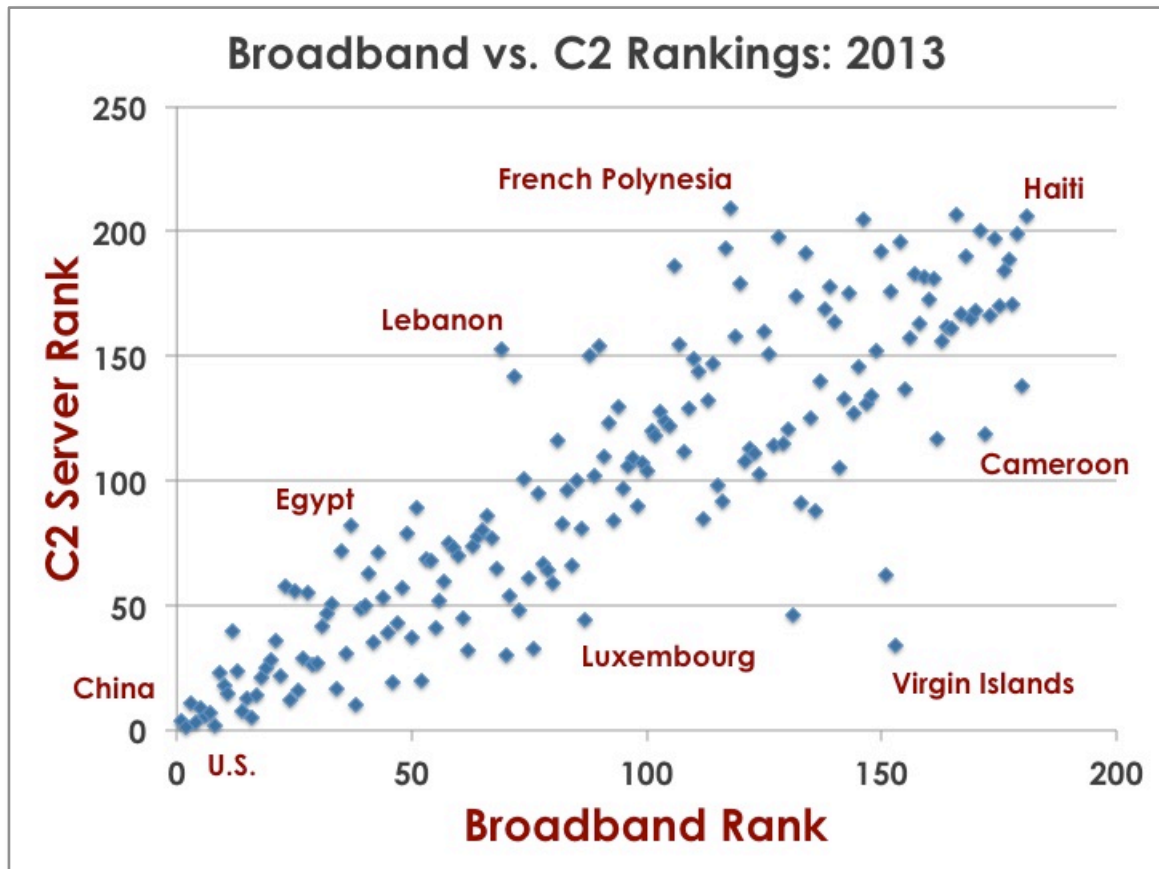
The chart below displays the unique number of callbacks per vertical in 1H 2014, by month.



Here, we can see that the world's callback infrastructure is dynamic, and at any given month, there are peaks and troughs in the extent to which hackers are communicating with compromised computers in any given vertical.

Connectivity and malware

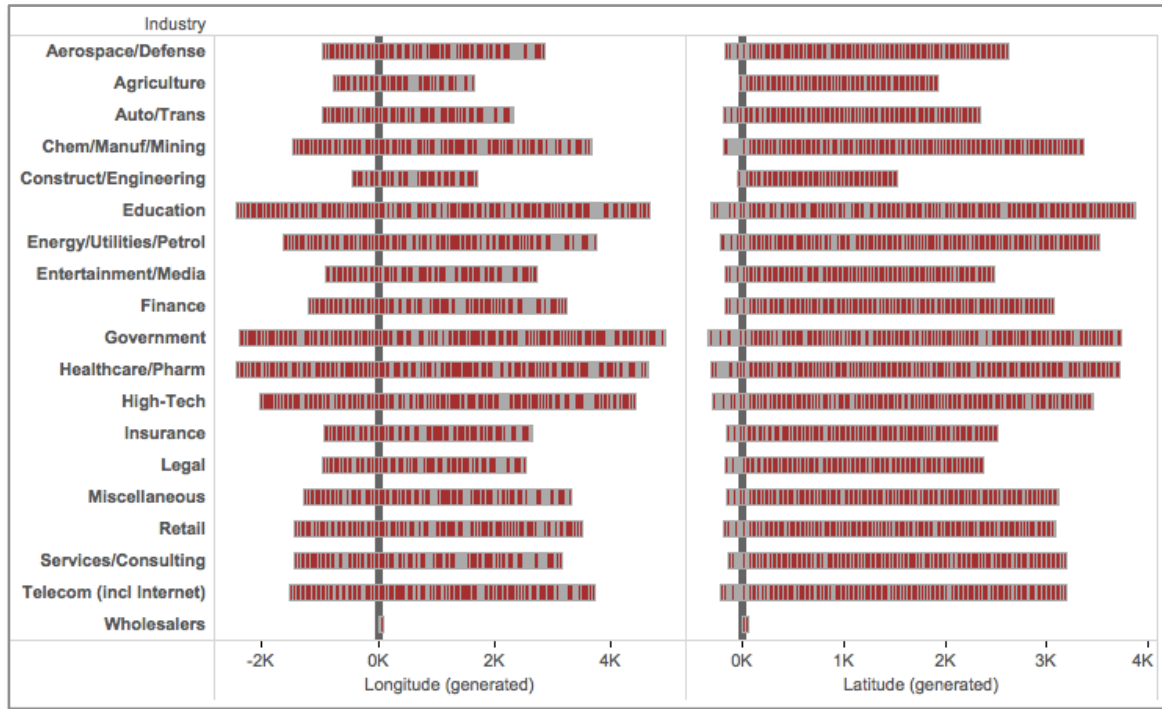
The graph below illustrates that some countries have a more acute malware problem than others. Here, the world's countries are ranked based on their level of broadband access, as well as their relative number of C2 servers, according to our 2013 dataset.



In general, there is a rough correlation between Internet connectivity and malware infrastructure. However, according to our data, the Virgin Islands have a bigger malware problem than French Polynesia, and Luxembourg has a bigger malware problem than Lebanon. Note that the U.S. and China are tops in malware and in connectivity, respectively.

Callbacks by vertical / country

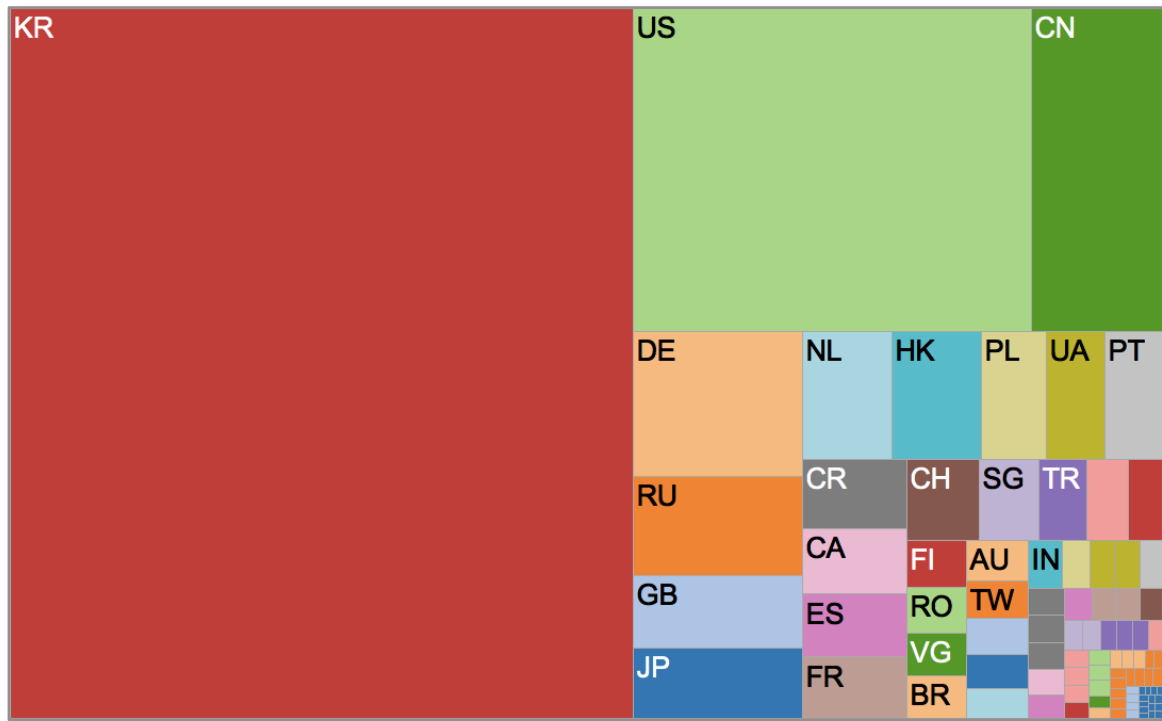
The chart below displays the location of C2 servers by longitude and latitude, divided by a combination of victim industry vertical and C2 server location. The red boxes represent industry verticals, such as *Insurance*, and their place in the chart indicates the country hosting their C2 servers, such as *India*.



Our data strongly suggest that the vast majority of C2 servers today are located above the Equator, and a preponderance of them are east of the prime meridian in Greenwich, England. Servers in the United States dominate the left side of the longitude graph.

Callback destinations from South Korea

In many countries, the top callback destination may be to other compromised networks within the same nation. Hackers often choose this strategy in order to decrease the potential suspicion of network security administrators, who routinely examine their log files for dubious connections.

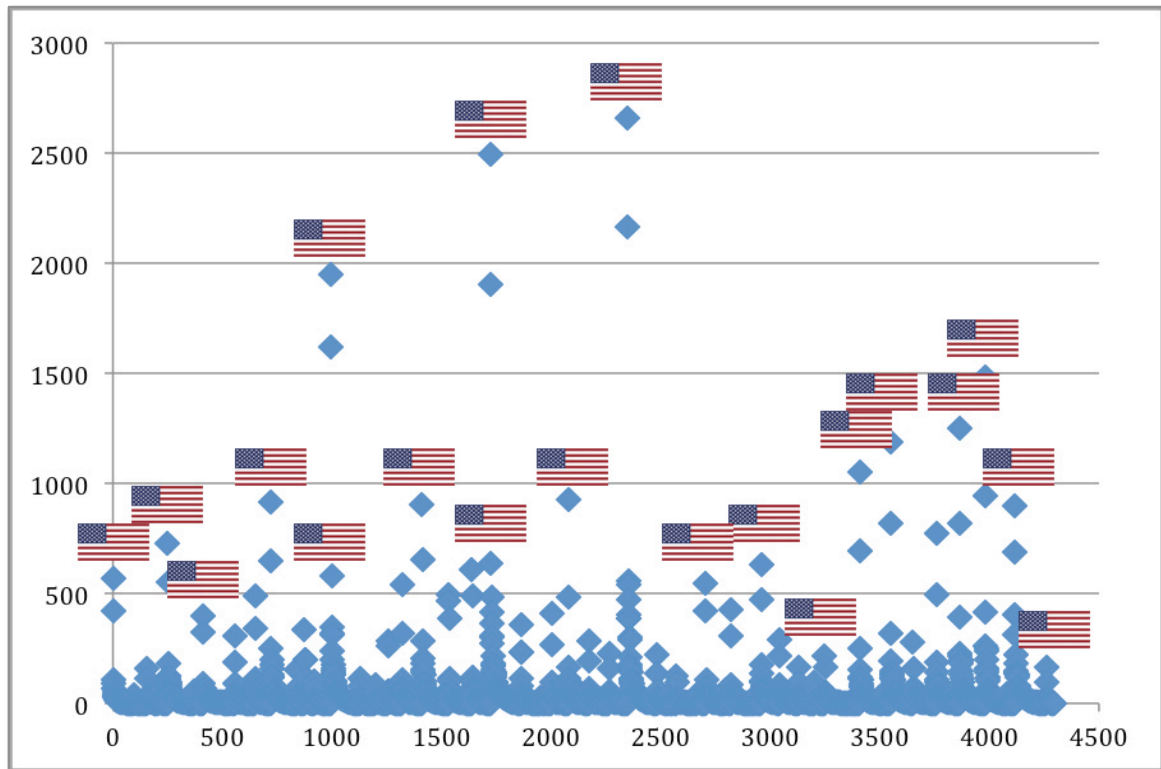


For our South Korean victim dataset, we can see that this may be the most common path for hackers in that country – roughly half of all callbacks were to other compromised South Korean computers.

USA: the top callback destination

The United States, however, hosts by far the highest single number of C2 servers in the world. Thus, it is also the world's most common callback destination.

The graph below clearly illustrates the central role that the U.S. now plays in the world's malware infrastructure. The horizontal axis represents over 4,000 FireEye clients from 73 countries; the vertical axis represents the number of C2 servers they reported to, by country.

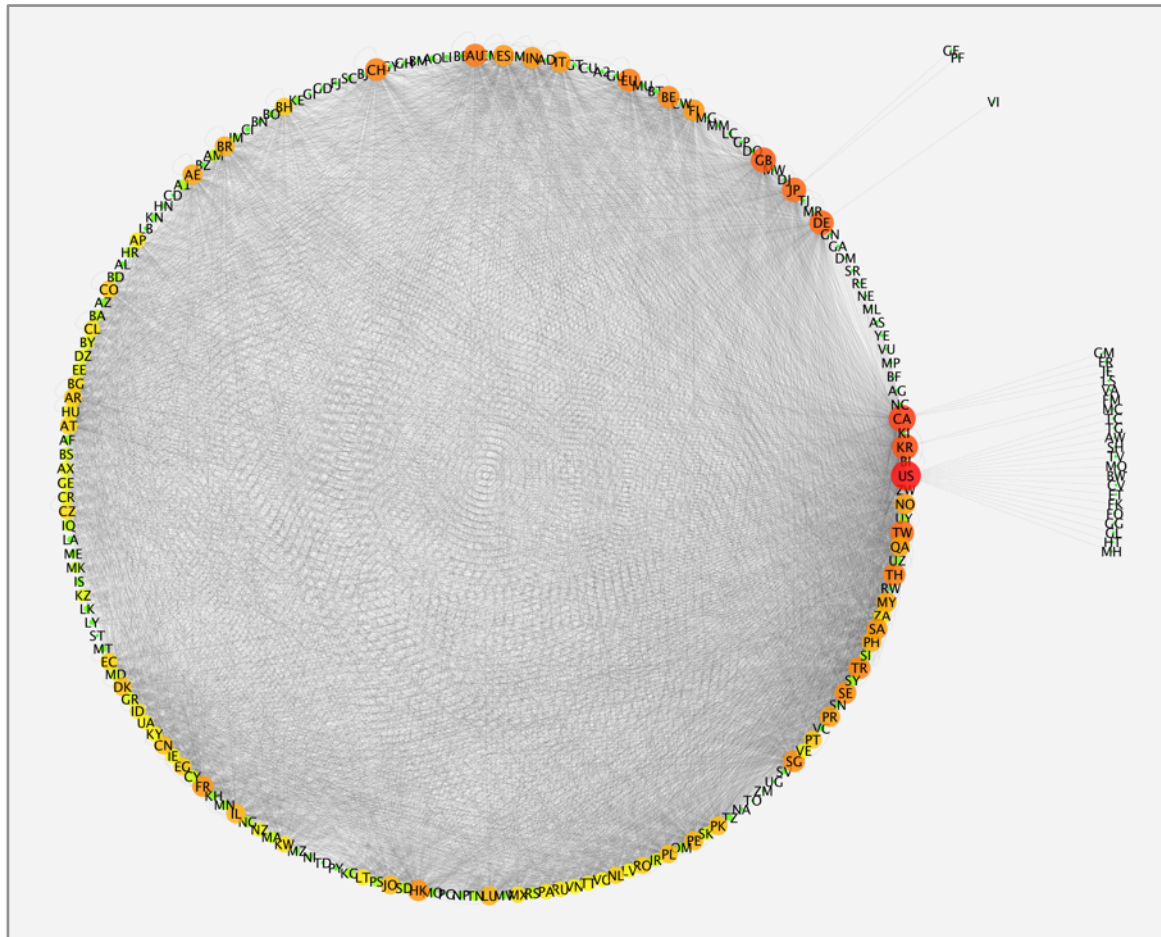


In nearly every case, the top callback destination (for most clients) are servers based in the U.S.

It is important to remember that this chart does not mean that the human attackers themselves are in the U.S. – merely that the first “hop” the attackers are leveraging is located in the U.S. The U.S. is the country with the most computers connected to the Internet, and most of the world's Internet traffic currently passes through the U.S. The true source of the attack, as we saw earlier in this paper, could be anywhere in the world.

World C2 network map

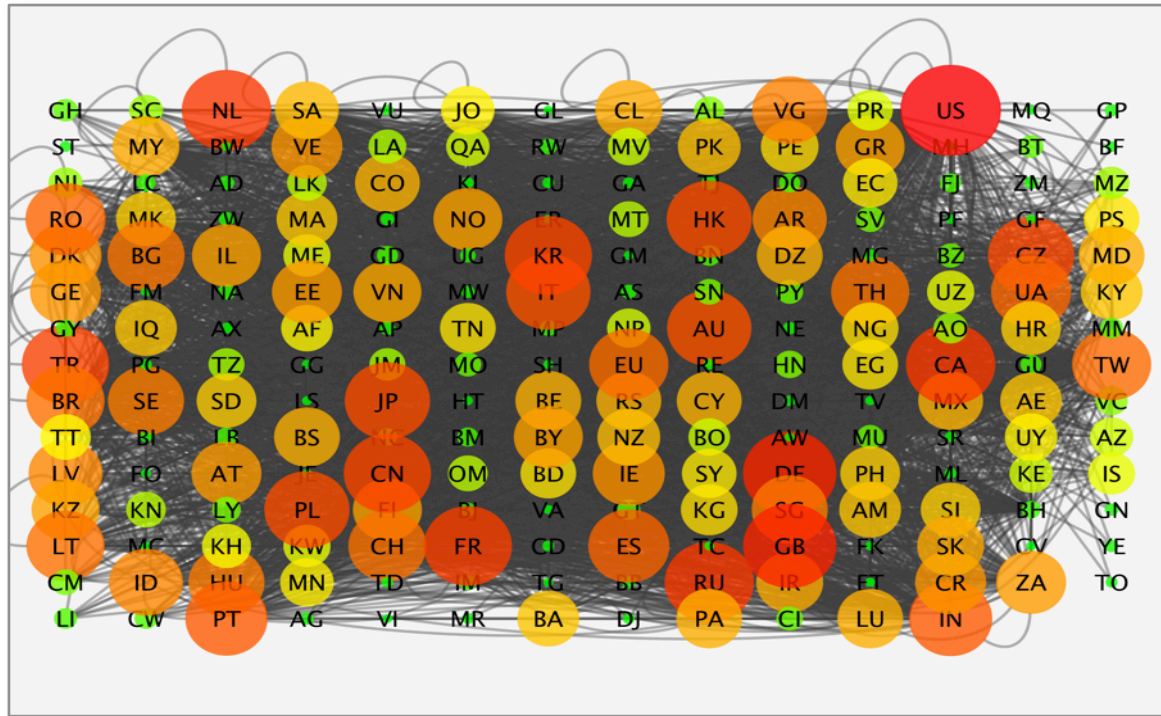
Let's zoom out again to look at the whole of Planet Earth, but this time from a network perspective. Here are the victims and their callback destinations from our 2013 dataset of over 22 million callbacks. In this chart, there are 208 countries and territories (nodes), and 4,719 malware callback connections between them (edges).



The centrality of the countries in this map of Planet Earth's callback infrastructure is signaled by node size and color. On the right side of the chart, you can see the relative importance of the U.S., South Korea, Canada, Germany, and Japan not only by these traits, but also by the fact that there were victim machines in some countries that called back to them exclusively (these are depicted on the far right side of the chart).

World C2 network heatmap

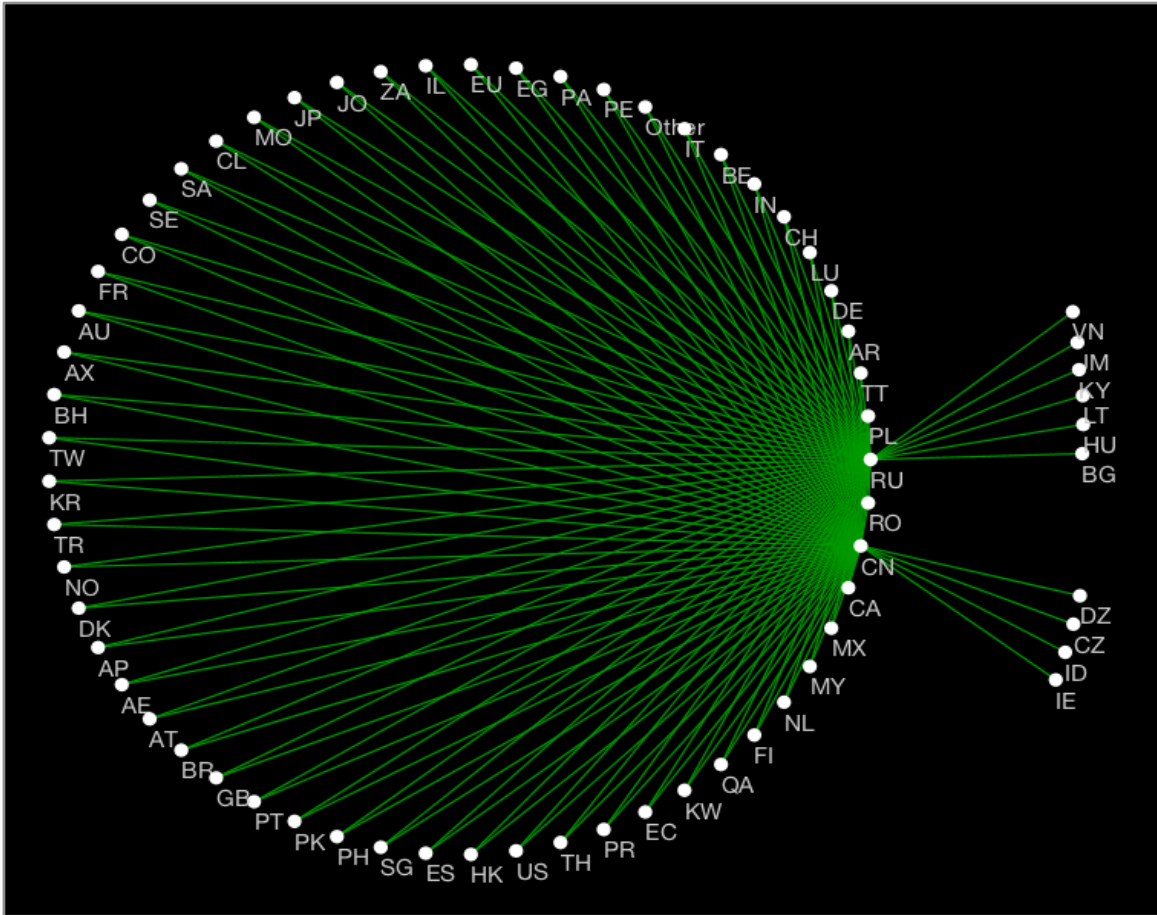
Here is a different, more legible network chart of the same data, with the exception that it magnifies the “indegree” of the edges, or the number of inbound malware connections (i.e. inward directed edges) to each country.



In this chart, the centrality of some countries rises considerably, including (from left to right) Turkey, Netherlands, Poland, Japan, China, France, Italy, Hong Kong, Russia, Czech Republic, and Ukraine. The indegree analysis signifies that these countries play a relatively more significant role in the world’s callback infrastructure (in terms of hosting C2 servers).

Overlap: investigative headache

If we isolate any two countries side-by-side, we are likely to see significant overlap in their callback infrastructure. The network chart below shows the countries with infected computers that we saw calling back to China and Russia.



For the most part, they are identical. However, there are a few unique countries reporting to each. To China, only one of the unique countries is in Asia (Indonesia), but in the case of Russia, three are located in the immediate, former Soviet sphere of influence: Lithuania, Hungary, and Bulgaria.

Case Study: Russia/Ukraine: Malware Callbacks Rise as Conflict Deepens

Cyber conflict is primarily a reflection of other, more “traditional” human conflicts. And the more serious the conflict in the “real world”, the more conspicuous its cyber shadow is likely to be. So let’s look at a serious, current international conflict – that between Russia and Ukraine – to see if we can find its reflection in cyberspace.

The table below shows the top 15 countries that received malware callbacks over the course of 16 months, according to FireEye data.

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
1	US	US	US	US	US	US	US	US	US	US	US	US	US	US	US	US
2	DE	KR	DE	DE	DE	KR	KR	KR	DE	DE	KR	KR	KR	KR	US	KR
3	KR	DE	KR	KR	KR	DE	DE	DE	KR	KR	DE	CN	CN	DE	RU	DE
4	CN	CN	CN	CN	NL	NL	GB	CN	CN	CN	CN	NL	DE	CN	DE	RU
5	RU	RU	HK	HK	RU	GB	NL	GB	GB	NL	NL	DE	FR	FR	CN	GB
6	FR	FR	FR	RU	GB	CN	CN	NL	CA	GB	GB	GB	RU	NL	GB	CN
7	NL	GB	NL	NL	CN	RU	CA	CA	NL	RU	CA	FR	NL	RU	NL	NL
8	GB	TR	RU	GB	CA	CA	RU	RU	RU	CA	RU	RU	GB	GB	FR	UA
9	JP	NL	CA	FR	FR	FR	JP	FR	TR	JP	FR	CA	CA	UA	UA	FR
10	PL	CA	TH	CA	HK	HK	PL	JP	FR	UA	UA	UA	UA	CA	CA	CA
11	CA	ID	GB	IT	IN	TR	FR	PL	UA	TR	JP	RO	PT	PT	HK	PL
12	IN	JP	BG	JP	UA	JP	HK	HK	JP	RO	TR	PL	RO	PL	PT	PT
13	RO	HK	TR	PL	PL	IT	UA	UA	PT	CZ	PT	PT	TR	JP	RO	JP
14	IT	UA	UA	UA	JP	PL	PT	CZ	IT	IE	AU	TR	PL	RO	TR	TR
15	UA	PL	JP	BG	TR	AR	IT	BR	CZ	FR	GE	IN	JP	TR	PL	RO
16	ID	RO	IT	TR	PT	UA	TR	IT	PL	PT	HK	JP	BR	CZ	JP	HK
17	HK	IN	PL	IN	BG	RO	VN	TR	HK	PL	PL	ES	CZ	BR	CZ	CZ
18	TW	PA	ID	TH	IT	IN	RO	PT	ES	IT	RO	AU	IT	IT	ES	IT
19	TR	IT	LT	TW	TH	AU	IN	AU	BR	SE	ES	EU	ES	ES	BR	BR
20	HU	TH	IN	CH	RO	BG	SD	TW	IN	HK	IN	HK	HK	HK	IT	TH
	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2014	2014	2014	2014

These data suggest that there is a significant correlation between the number of callbacks to each country and the expansion of the crisis between Russia and Ukraine.

In 2013, Russia was on average #7 on this list; in 2014, its average rank is #5.

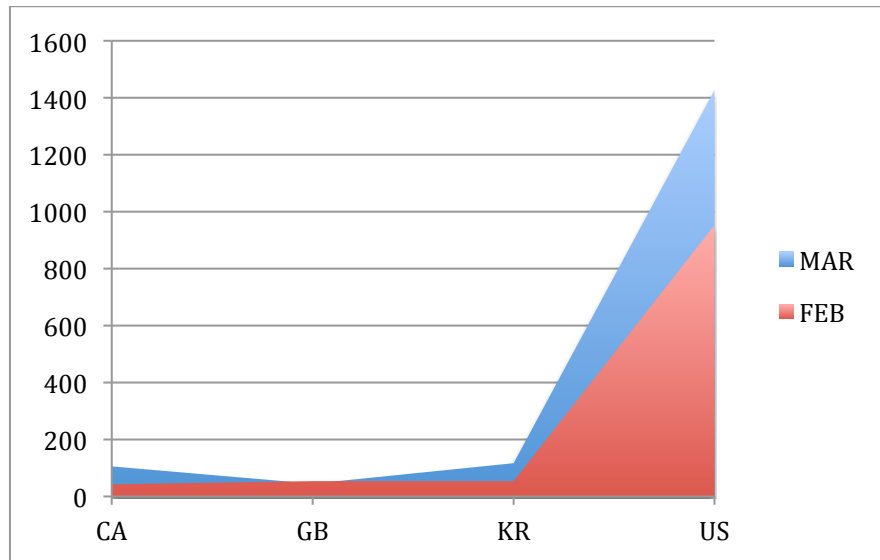
In 2013, Ukraine was on average #12 on this list; in 2014, its average rank is #9.

The biggest single monthly jump occurred in March 2014, when Russia moved from #7 to #3. In that same month, [the following events](#) also took place in Russia and Ukraine:

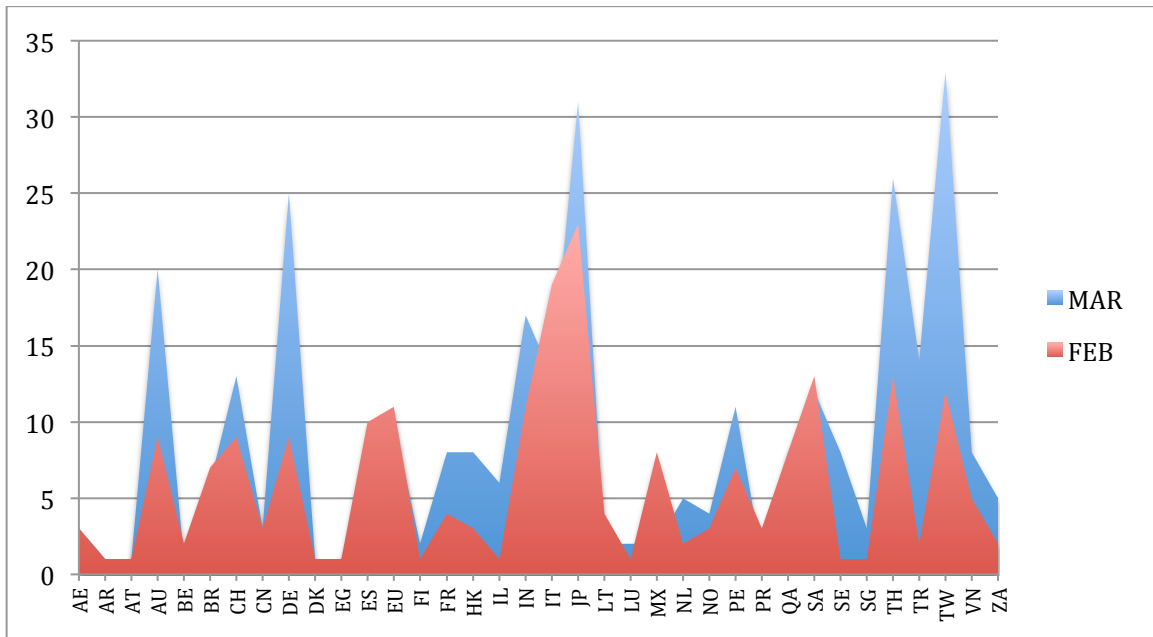
- Russia’s parliament authorized the use of military force in Ukraine;
- Vladimir Putin signed a bill incorporating the Crimean peninsula into the Russian Federation;
- the U.S. and EU imposed travel bans and asset freezes on some senior Russian officials;
- Russian military forces massed along the Ukrainian border; and
- Russian energy giant Gazprom threatened to cut off Ukraine’s supply of gas.

The graphs below provide a closer look at the critical month of March, specifically comparing it to the data from February.

In March 2014, there was a clear rise in callbacks to Russia from three of the top four source countries from February: Canada, South Korea, and the U.S. (Great Britain had a slight decline).

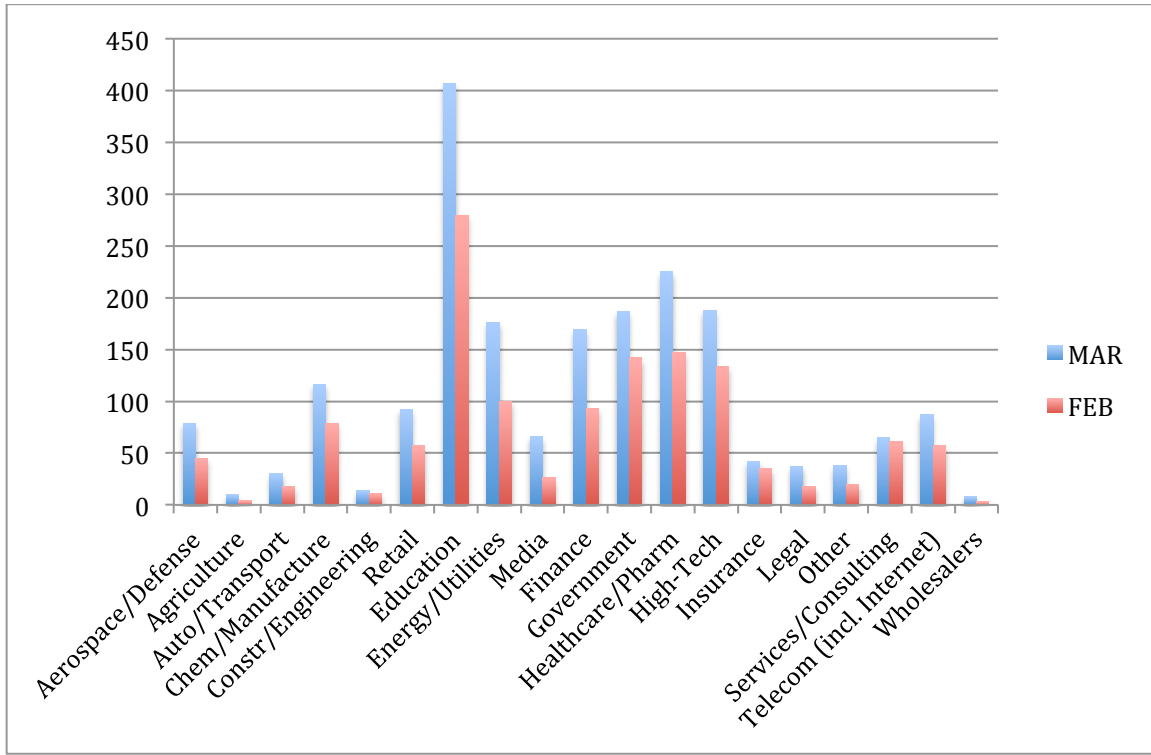


The following graph demonstrates that there was a general rise in callbacks to Russia from many other countries around the world.



The primary reason for this could be that hackers are able to communicate with a wide variety of the compromised infrastructure to which they have access, at will, and that they likely spread their operations out over a wide variety of networks in an effort to avoid detection and mitigation by network security administrators.

The following graph provides further evidence to support this hypothesis; the rise in callbacks to Russia in March 2014 could be seen in every industry vertical.



In an effort to cross-examine these conclusions, the tables below compare the relative rise and fall in callbacks from Russia and Ukraine to all other countries in the world for February and March 2014.

The first table lists the countries that received the highest increase, from February to March 2014, in the number of source countries sending callbacks to them. Russia and Ukraine both placed in the top ten countries worldwide.

Rank	Country	FEB	MAR	Δ
1	HR	6	18	+12
2	LT	18	30	+12
3	IL	9	19	+10
4	UA	29	39	+10
5	RO	25	34	+9
6	ES	27	35	+8
7	RU	45	53	+8
8	AF	4	11	+7
9	SI	2	9	+7
10	TR	29	36	+7

The table below shows the difference in the number of malware signatures associated with the callbacks to each country, for February and March 2014. Ukraine does not appear in the top ten (it tied for #15, which is still very high considering that we analyzed C2 traffic to 208 country and territory top-level domains (TLD)), but Russia placed #4 in the world during this time period.

Rank	Country	FEB	MAR	Δ
1	US	725	847	+122
2	CN	164	201	+37
3	HK	77	113	+36
4	RU	109	142	+33
5	NL	106	129	+23
6	DE	164	179	+15
7	TR	43	57	+14
8	TH	23	36	+13
9	DK	18	30	+12
10	SG	25	35	+10

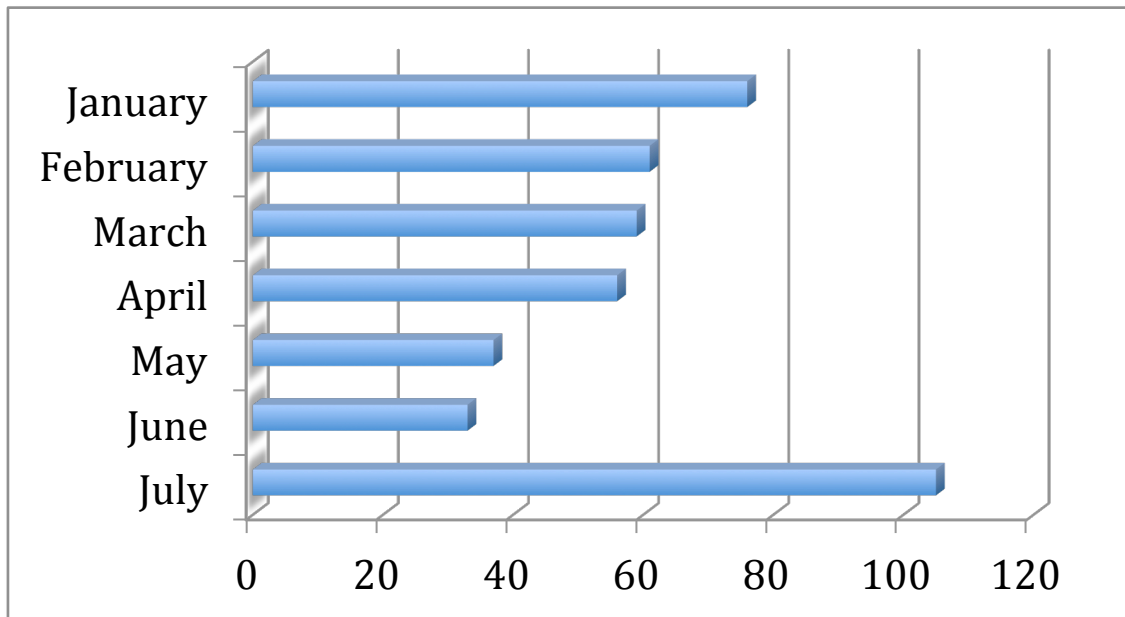
To summarize this case study, we believe that the rise in callbacks to Russia and Ukraine during the first four months of 2014, simultaneous to the expansion of the conflict on the ground, demonstrates that computer network operations are being used as a way to gain competitive advantage in this real world conflict.

Again, to arrive at this conclusion, it is not necessary to know the real world identity of any one attacker, or his or her precise motive. This is strategic analysis.

Geopolitical reflection: Israel-Gaza crisis

Any successful experiment needs to have results that can be duplicated in subsequent tests. In an effort to repeat the results we found for the conflict in Ukraine, all we needed was to correlate worldwide callback data with an acute international crisis.

The current conflict between Israel and Gaza in July 2014 gave us this opportunity. The graph below shows the number of unique callbacks sent to Israel in 2014, according to FireEye data.¹



The dramatic jump in C2 traffic to Israel during the month of July 2014 coincided with [Israel's military campaign in Gaza](#).

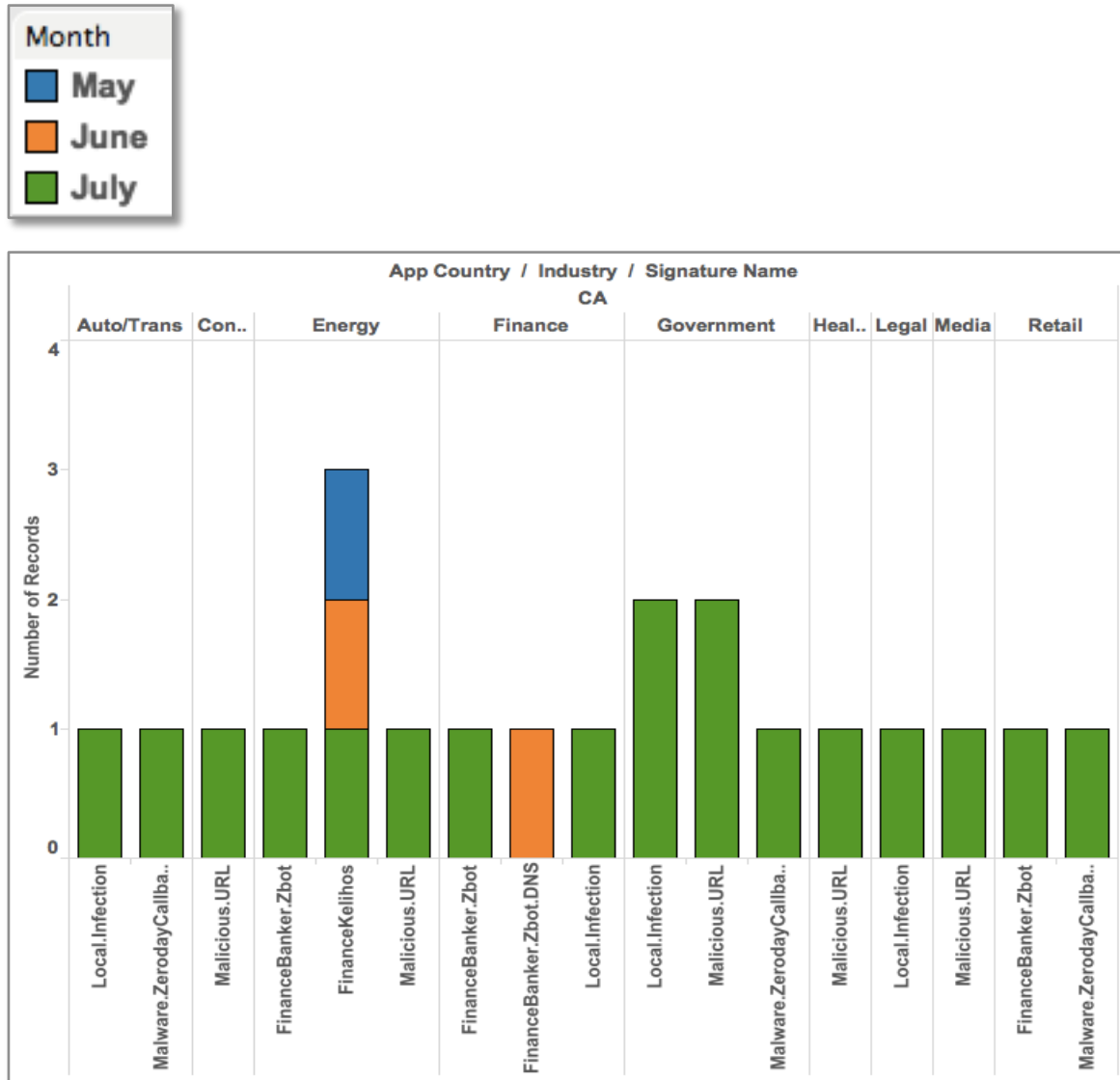
We believe that this finding is roughly similar to the dynamic we observed in Ukraine and Russia during their conflict this year – that computer network operations are now being used as a way to gain advantage in a political-military conflict.

We are able to discover this evidence only because FireEye now has access to a truly strategic dataset.

¹ We examined data through July 21, 2014, and extrapolated the numbers to July 31 based on the trend up to July 21.

Unique callbacks: CA to IL (2014)

There was, however, an interesting difference between the Russia/Ukraine callbacks and the callbacks to Israel. Instead of being spread out over many countries, the rise in callbacks to Israel was easy to isolate – they came primarily from the U.S. and Canada (however, they were spread out across verticals). The C2 communications from Canada were the most significant from a statistical perspective, as seen in the chart below.



At FireEye, we caught only one unique callback from Canada to Israel in May and two in June ... but we found eighteen (18) in July! And three of the July callbacks were associated with zero-day malware signatures. 😊

Conclusion

Over the past 18 months, FireEye observed over 30 million malware callbacks sent to over 200 countries and territories. From this strategic dataset, the authors have employed high-level traffic analysis to shed light on how this Leviathan of malware is used to gain advantage in traditional geopolitical conflicts.

This is only a small step toward improving cyber attack attribution, as C2 servers remain only a first “hop”, or a first stage, in a longer chain of compromised computers that can anonymize any single attacker’s true location, identity, and motive.

However, this research is not about the attribution of any single attack, but it is a study of how the strategic volume, frequency, and direction of thousands and millions of callbacks can be correlated to traditional geopolitical events.